The URL Cruise Missile:

1. Parameter
2. Path
3. A disgruntled employee, retail competitor and hackers looking for a bargain
4. Any present exploit can be a target of injection
5. Confidentiality
6. Developers can secure parameters. Keeping everything up to date with security patches. Principle of least privilege

Web Server Infrastructure

1. Database stores the confidential information
2. Web Application
3. Web Server
4. Client
5. Firewall

Server Side Attacks

1. Input sanitation
2. Validation
3. High costs, developer oversight, lack of foresight
4. An individual can simply bypass robots.txt to browse blocked directories
5. You can choose a better domain provider and protect the domain control panel
6. False. Client side is more prone to unknown vulnerabilities because the client user may not be as informed on security matters as a security professional thus presenting many more vulnerability variables.

Web Application Firewalls

1. Layer 7: Application
2. WAFs filter/monitor web traffic and attempt to guard against attacks such as SQL injection and cross-site-scripting.
3. True

Authentication and Access Controls

1. The four factors are knowledge, possession, inherent and location based. Knowledge factors are memorization based and include the likes of passwords, passphrases and pins. Possession factor embodies a lock and key symbol and an example could be a security token. Inherent factors (biometrics) usually authenticate through voice, fingerprint, facial recognition and iris scanning. Finally, Location based authentication is reliant on GPS services.
2. False. Both are based on the same factor (knowledge).
3. True. Google authenticator is a form of security token (software based).
4. A constrained user interface restricts specific privileges that are based on clearance.